Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233

COMMENTS OF HUAWEI TECHNOLOGIES CO., LTD.,

AND HUAWEI TECHNOLOGIES USA, INC.

Dennis J. Amari
Vice President, Federal & Regulatory Affairs

Donald A. (Andy) Purdy, Jr.
Chief Security Officer

Huawei Technologies USA, Inc.
1101 16th Street, NW., Suite 401
Washington, DC 20036

Andrew D. Lipman
JiaZhen (Ivon) Guo

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
ivon.guo@morganlewis.com

Counsel to Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc.

September 20, 2021

SUMMARY

The Commission's proposed rules seek to (1) prohibit authorization of virtually all Huawei radio frequency ("RF") equipment under the equipment authorization rules, and (2) revoke previously issued equipment authorization of Huawei RF equipment. The Commission lacks any factual basis to justify the proposed rules to extend the prohibition on equipment authorization to all devices produced by Huawei, disregarding any of the technical criteria set forth under the existing equipment authorization rules. The Commission also lacks the authority to revoke existing authorizations already issued to Huawei equipment. Adopting the proposed rules would be arbitrary and capricious and therefore, unlawful. Instead of revoking equipment authorization based on the identity and country of origin of the equipment, the Commission should take a holistic approach to implement a cybersecurity framework.

The existing equipment authorization rules require the Commission to make factual, technical, and rational decisions in issuing authorizations. The Commission has no evidence that Huawei has violated any of these rules. Huawei's equipment has been recognized by independent third parties, world leading carriers, major enterprise and industry customers as being of the highest technical quality. The identity of a manufacturer, by itself, cannot rationally be connected to any of the purposes of the equipment authorization rules.

The proposed rules also cannot be supported by a cost-benefit analysis. The rules would impose substantial costs on carriers, end-users, distributors, suppliers, and resellers of Huawei equipment. Revoking existing equipment authorizations and prohibiting new ones would require these United States entities to divert limited resources, threaten service quality, and increase the cost of service, without equivalent benefits.

The proposed rules exceed the Commission's statutory authority to impose technical standards. The equipment authorization rules were adopted pursuant to express statutory provisions that

deal with technical issues, and (absent a specific directive as in the Anti-Drug Abuse Act) the Commission cannot prohibit the importation, marketing, or sale of a company's products based on the identity of the manufacturer without regard to the technical characteristics of a particular product.

The proposed rules are not supported by the Communications Act, the Communications Assistance for Law Enforcement Act, or any other statutory authority. Section 302 of the Communication Act only authorizes the Commission to make reasonable regulations governing RF emissions to prevent interference to lawful users of spectrum resources. The Commission's other statutory responsibilities under Sections 303(e) and 303(g) of the Communications Act do not authorize the Commission to withhold or revoke equipment authorizations based on national security considerations. The Communications Assistance for Law Enforcement Act was adopted to enact specific processes and protections for U.S. law enforcement wiretap and, therefore, cannot provide the Commission a possible source of authority. Furthermore, the Commission cannot assert ancillary jurisdiction because the Secure Networks Act reflects an explicit Congressional intent to prohibit the direct or indirect use of specific Federal subsidies through a program administered by the Commission to purchase covered equipment or services used by providers of advanced communications service. The Secure Networks Act does not give the Commission general jurisdiction to regulate any other use of covered equipment or services.

The proposed rules raise additional constitutional concerns as the prohibition and revocation mandate would cause due process violations and unlawful primary and secondary retroactivity. The proposed rules would violate Huawei's Due Process rights by depriving the company of its constitutionally protected property without minimal procedural protections. The proposed rules would also impose primary retroactivity and unreasonable secondary retroactivity. Revocation of

authorizations that were properly issued under the existing rules would impose a new disability based on past conduct, rendering the rule impermissibly retroactive in the primary sense. It also would adversely and unreasonably alter the future legal consequences of past actions by making Huawei's RF equipment essentially useless, rendering the rule impermissibly retroactive in the secondary sense as well. Additionally, the proposed rules would violate the Bill of Attainder Clause by singling out Huawei for punishment.

Instead of focusing solely on the origin of equipment vendors and adopt categorical bans, Huawei advises the Commission to adopt more reasonable alternatives, such as the use of a more fact-based holistic approach to cybersecurity. Experts across the United States government, including the National Institute of Standards and Technology; the Communications Security, Reliability, and Interoperability Council; and the White House, as well as industry participants, have all voiced the support of a framework based on multi-stakeholder collaboration, rather than unilateral categorical bans. Because the Commission's inquiries into enhancing cybersecurity are not new, it should leverage prior efforts to build upon existing works contributed by industry leaders to address the particular cybersecurity risks.

For these reasons, the Commission should reject the proposed rules.

Table of Contents

Page

I. INTRODUCTION 1

II. THE COMMISSION LACKS ANY FACTUAL BASIS TO JUSTIFY THE PROPOSED RULES, AND IT IS THEREFORE ARBITRARY AND CAPRICIOUS TO ADOPT THE PROPOSED RULES. 3

A. The Commission Is Required to Make Rational and Factual Decisions Based on Technical Considerations. 4

B. There is No Evidence of Huawei's Violation of the Existing Equipment Authorization Rules. 6

C. Huawei's Equipment Has Been Recognized by Independent Third Parties, World Leading Carriers, Major Enterprise and Industry Customers as Being of the Highest Technical Quality. 10

D. The Commission's Proposal Cannot Be Justified by a Cost-Benefit Analysis. 15

III. THE COMMISSION LACKS STATUTORY AUTHORITY TO ADOPT THE PROPOSED RULES. 18

A. The Proposed Rules Exceed the Commission's Authority to Impose Technical Equipment Standards. 19

B. No Statute Explicitly Gives the FCC Any Discretion to Withhold or Revoke Equipment Authorizations Based on National Security Considerations Regardless of the Equipment's Compliance with Technical Standards. 22

1. Section 302 of the Communications Act Cannot Provide the Authority. 22

2. Section 303 of the Communications Act Also Does Not Authorize the Commission's Proposed Rules. 25

3. The Communications Assistance for Law Enforcement Act Can Not Provide A Source of Authority. 27

C. The Commission also lacks ancillary authority to promulgate the proposed rules. 30

IV. THE PROPOSED RULES ARE UNCONSTITUTIONAL AND VIOLATE THE ADMINISTRATIVE PROCEDURE ACT. 34

A. Revocation of Existing Authorizations Would Constitute Regulatory Taking of Property Interests Without Due Process Protection. 34

B. The Proposed Rules Would Violate the Bill of Attainder Clause by Singling Out Huawei For Punishment. 36

Table of Contents
(cont'd)

Page

C. The Proposed Rules Would Violate the Administrative Procedure Act by Imposing Primary Retroactivity and Unreasonable Secondary Retroactivity..... 36

V. THE COMMISSION SHOULD LOOK TO EXISTING PROGRAMS AND FRAMEWORKS TO STRENGTHEN CYBERSECURITY. 38

A. The U.S. Government, Expert Advisors to the Commission, and Industry Agree That a Risk-Management Approach to Security Is More Appropriate Than Categorical Bans on Certain Providers. 39

B. The Commission's Inquiries into Enhancing Cybersecurity and Security-by-Design for 5G Networks Are Not New. 48

C. The Commission Should Leverage Prior Efforts to Build and Enhance Cybersecurity and Address the Particular Security Risks..... 51

VI. CONCLUSION..... 53

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233

COMMENTS OF HUAWEI TECHNOLOGIES CO., LTD., AND HUAWEI TECHNOLOGIES USA, INC.

Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc. (collectively, "Huawei"), by their undersigned counsel, submit these comments to the Federal Communications Commission ("FCC" or "Commission") in response to the Notice of Proposed Rulemaking ("NPRM") and Notice of Inquiry ("NOI"), FCC 21-73, released in ET Docket No. 21-232 and EA Docket No. 21-233 on May 27, 2021 and published in the Federal Register on August 19, 2021, at 86 Fed. Reg. 46641.[1]

I. INTRODUCTION

Huawei responds to the Commission's NPRM, which proposes to (1) prohibit all future authorizations for equipment on the list of equipment and services ("Covered List") that the Commission maintains pursuant to the Secure and Trusted Communications Networks Act of 2019

[1] *See Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, Notice of Proposed Rulemaking and Notice of Inquiry, ET Docket No. 21-232, EA Docket No. 21-233, FCC 21-73 (rel. Jun. 17, 2021) ("NPRM and/or NOI").

("Secure Networks Act"),[2] (2) prohibit entities named on the Covered List from using the Supplier's Declaration of Conformity ("SDoC") procedure at all, even for equipment that is not specified on the Covered List,[3] (3) permit the Commission to revoke authorizations that have been previously granted for equipment on the Covered List,[4] and (4) require participants in Commission auctions to certify that their bids do not rely on financial support from any entity that has been designated as a national security threat.[5] The Commission has also asked for comment on whether it should no longer provide an exemption to equipment on the Covered List that would otherwise be exempt from the equipment authorization requirements due to its low level of radio frequency ("RF") emissions.[6]

The Commission cannot and should not adopt the proposed rules and should terminate the NPRM for several reasons. *First*, the Commission's proposed rules lack a rational and factual basis and arbitrarily and capriciously treat Huawei differently from other similarly situated companies manufacturing RF equipment. *Second*, the Commission lacks statutory authority to prohibit equipment authorizations from being issued to Huawei equipment that is not causing RF interference. The Commission also lacks authority to revoke equipment authorizations already issued to Huawei equipment that still complies with the technical standards set forth under the equipment authorization rules. *Third*, even if the Commission had authority, which it does not, the Commission's proposal would violate the U.S. Constitution, the Administrative Procedure Act ("APA"), and the Communications Act.

---

2 *See* NPRM, ¶¶ 44-56; *see also* NPRM, App. A (proposed § 2.903).

3 *See* NPRM, ¶¶ 57-64; *see also* NPRM, App. A (proposed §§ 2.906, 2.907).

4 *See* NPRM, ¶¶ 80-89.

5 *See* NPRM, ¶¶ 90-97.

6 *See* NPRM, ¶ 76.

Huawei further responds to the Commission's NOI, which seeks to leverage the equipment authorization program to encourage network device manufacturers to consider cybersecurity standards and guidelines.[7] Huawei appreciates the opportunity to share its views and experiences related to implementing a holistic cybersecurity framework with the Commission. Cybersecurity is a distinct priority for Huawei and should be a priority concern for *all* equipment in the telecommunications network, regardless of its manufacturer or country of origin. The Commission should renew and extend prior efforts by industry associations, enterprises, and individual customers to promote cybersecurity best practices so that U.S. communications networks will be reliable and appropriately secure.

II. THE COMMISSION LACKS ANY FACTUAL BASIS TO JUSTIFY THE PROPOSED RULES, AND IT IS THEREFORE ARBITRARY AND CAPRICIOUS TO ADOPT THE PROPOSED RULES.

The NPRM proposes to adopt a new subsection as part of the Commission's rules to impose "a clear prohibition" on equipment authorizations concerning any equipment on the Covered List,[8] regardless of the authorization process to which that equipment currently is subject.[9] Specifically, the Commission proposes to adopt a new subsection 2.903, as part of the "General Provisions" of Part 2, Subpart J, to prohibit any equipment on the Covered List from obtaining an equipment authorization, including equipment subject to the Commission's certification procedures and SDoC procedures.[10] It also proposes to prohibit any entity named on the Covered List, such as

---

7 NPRM, ¶¶ 98-105.

8 47 CFR § 1.50002.

9 NPRM, ¶ 41.

10 NPRM, ¶¶ 41-69.

Huawei, from using the SDoC process for *any* equipment, regardless of whether it is on the Covered List.[11] The NPRM also seeks comment on whether any other changes to Subpart I or K rules are needed to effectuate its intention to prohibit the marketing and importation of such equipment.[12]

In doing so, the Commission proposes to ban equipment based solely and exclusively on the identity of its manufacturer rather than any technical considerations under the existing equipment authorization rules. The Commission's proposed rules are too indiscriminate and lacking in a factual basis to survive judicial review. Such a revised set of rules would be arbitrary and capricious and therefore unlawful.

A. The Commission Is Required to Make Rational and Factual Decisions Based on Technical Considerations.

In a departure from its long-standing support for a risk-management approach, the Commission proposes banning authorization of equipment from companies identified on the Covered List, without any particularized finding that any specific piece of equipment poses any risk of any harm to anyone.[13] The Commission states its proposed rules are intended to "establish a clear prohibition on the authorization of any 'covered' equipment in [the] equipment authorization processes regardless of the process to which that equipment is subject."[14] Imposing a categorical prohibition on equipment based on the identity, even if such equipment meets all relevant technical criteria, would be *per se* arbitrary and capricious.

---

[11] NPRM, ¶¶ 73-79.

[12] NPRM, ¶ 42.

[13] NPRM, ¶¶ 40-72.

[14] NPRM, ¶ 41.

As the Commission readily conceded, the equipment authorization program is designed to "ensure that RF devices imported to or marketed within the United States comply with the Commission's *technical requirements*."[15] Although the program has undergone multiple revisions in the past decades to account for technical and procedural changes,[16] the cornerstone of the program remains a technical one.[17] Indeed, the basis and purpose of the Commission's equipment authorization rules as stated in Part 2, Subpart J, is "to promote efficient use of the radio spectrum" and in order to do that, "the Commission has developed *technical standards* for radio frequency equipment and parts or components thereof."[18] These technical standards include specific and detailed criteria applicable to individual types of equipment.[19]

Rather than adopting a rule to regulate the RF devices based on technical standards, the Commission proposes to prohibit the authorization of any equipment on the Covered List, irrespective of whether the equipment is subject to the existing certification or SDoC procedures. However, Congress directed the Commission to create the Covered List for the specific purpose of identifying equipment that should not be used in carrier networks supported by Universal Service Fund ("USF") payments. The Commission fails to offer a sufficient justification for extending this ban beyond the Covered List's intended purpose. There is no rational basis for assuming that simply because equipment is on the Covered List its use in the United States would interfere in

---

15 NPRM, ¶ 24 (emphasis added).

16 *See, e.g.*, *Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules Regarding Authorization of Radiofrequency Equipment*, First Report and Order, ET Docket No. 15-170, 32 FCC Rcd 8746 (2017).

17 *See, e.g.*, 47 CFR §§ 2.1046 (measuring RF power output), 2.1047 (modulation characteristics), 2.1049 (occupied bandwidth), 2.1051 (spurious emissions at antenna terminals), 2.1053 (field strength of spurious radiation), 2.1055 (frequency stability), 2.1057 (frequency spectrum).

18 47 CFR § 2.901 (Basis and Purpose) (emphasis added).

19 47 CFR § 2.901(a); *see also* 47 CFR Part 15 (rules governing individual types of equipment).

any way with the effective use of the radio spectrum or violate any of the technical criteria in Subpart J. Addition to the Covered List does not take into account any technical considerations. Instead, as Huawei's Comments in other related proceedings established, Huawei's designation on the Covered List was primarily motivated by impermissible, unverified, unproven, unspecified, and unrelated allegations.[20]

Motivations aside, the proposed rules, if adopted, would contravene the Commission's own policy in certifying communications equipment. For example, in *Transportation Intelligence*, the Commission argued to the Court of Appeals that "i[n] certifying equipment, the Commission's primary concern is the *technical performance* of the equipment — whether it is capable of complying with the applicable *technical standards* and whether it is unlikely to interfere with other uses of the radio spectrum."[21] The Commission cannot arbitrarily and capriciously change course to promote a rule under which technical performance of the equipment is ignored and has no bearing.

B. There is No Evidence of Huawei's Violation of the Existing Equipment Authorization Rules.

The Commission also lacks any evidence in the record relating to Huawei and the current equipment authorization rules to sustain its proposals. Notably, the NPRM fails to identify any evidence of any actual harm or even potential harm to radio communications from the use of Huawei equipment. The Commission neither provides a single example of equipment manufactured by Huawei that has caused any technical issues for its users or for other persons operating

[20] *See* Comments of Huawei, PS Docket No. 19-351, at 57-82 (filed Feb. 3, 2020) ("Huawei Designation Comments").

[21] *Transportation Intelligence, Inc. v. Federal Communications Commission*, No. 02-1098, Appellee's Br. at 13-14, 2003 WL 25586291 (D.C. Cir. 2003) (emphasis added).

lawfully authorized equipment, nor does it even attempt to provide a rational, factual basis to suggest that Huawei would produce any such equipment in the future. Indeed, the United States government has not raised a single concern to Huawei or its customers regarding any Huawei products allegedly interfering with RF communications networks. On the contrary, the reality is that Huawei's equipment has never been found in violation of the Commission's equipment authorization rules and there has been no enforcement action against Huawei for any past or current violations.

Further, the proposed rules would explicitly and deliberately ban the use of Huawei equipment that is *known* not to pose any risk of harm. Even if Huawei could, as it has already consistently done in the past for all its RF equipment, demonstrate with scientific and technical certainty that a particular item of equipment complied with all applicable requirements and posed no potential harm of any kind, Huawei still would not be permitted to obtain an authorization for that item.

Prohibiting equipment authorization of all Huawei devices, including inherently secure equipment, would not improve security in any meaningful way. Much of the RF equipment subject to the Commission's proposed rules cannot cause any harm that the Commission seeks to prevent—interference to other users of the radio spectrum or to the networks that the rules purportedly seek to protect. Indeed, the existing equipment authorization rules exempt several types of products that, in the Commission's own words, "have virtually no potential for causing harmful interference to [t]he authorized radio services."[22] Therefore, this equipment could produce limited, if any, damage even if (hypothetically) corrupted, insecure or untrustworthy. Although the Commis-

[22] NPRM, ¶ 31; *see also* NPRM, ¶ 73.

sion never states what benefit it expects to achieve by prohibiting Huawei from importing or marketing equipment that has such limited potential to do any harm, the purpose of this proposal *cannot* be rationally related to the technical basis of the equipment authorization rules.

Revocation of equipment authorizations previously granted through certification or SDoC procedures without regard to technical considerations would also be legally unsupportable. To be sure, the existing equipment authorizations rules do contemplate that the Commission may revoke equipment authorizations for certain reasons, but none of those are applicable in this situation. Specifically, the Commission may revoke an authorization "[f]or false statements or representations either in the application or in materials or response submitted in connection therewith" or in records that the responsible party is required to maintain about the authorized equipment;[23] "[i]f … the equipment does not conform to the pertinent technical requirements or to the representations made in the original application[;]"[24] "[i]f … changes have been made in the equipment other than those authorized by the rules or otherwise expressly authorized by the Commission[;]"[25]

[23] 47 CFR § 2.939(a)(1).

[24] *See* 47 CFR § 2.939(a)(2).

[25] *See* 47 CFR § 2.939(a)(3).

"[b]ecause of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application[;]"[26] or in the event of changes in technical standards.[27]

But revocation of equipment authorizations is only permitted when there is clear and convincing evidence of egregious misconduct by the registrant (*e.g.*, false statement or misrepresentation, nonconformity to technical requirements, unauthorized changes to the equipment) or where there are changes in technical standards.[28] Here, there is neither any allegation of any misconduct by Huawei or violation of rules that were in effect at the time authorizations were granted; nor is there any change in *technical* standards that alters the interference potential of any equipment. A change in policy towards Huawei and the other companies named on the Covered List is not a change in "technical standards," and the Commission cannot make it so by fiat.

---

[26] *See* 47 CFR § 2.939(a)(4). This provision is based on Section 312(a)(2) of the Communications Act, permitting revocation of station licenses. The Commission has relied on "conditions . . . which would warrant it in refusing to grant an original application" only in cases of post-licensing misconduct; not based on facts that were known to the Commission before granting the license but not then considered grounds for denial. *See, e.g., KWK Radio, Inc. v. FCC*, 337 F.2d 540 (D.C. Cir. 1964) (licensee had conducted two treasure hunts in a manner which constituted deliberate fraud upon the public); *Theodore E. Sousa*, 92 FCC 2d 173 (1982) (distinguishing between facts presented in an application and facts otherwise known to some branch of FCC staff); *Theodore E. Sousa*, 93 FCC 2d 1064 (Rev. Bd. 1983) (revoking Citizens Band license based on repeated violations of Commission rules that would justify denial of an initial license application); *Roger Thomas Scaggs*, 19 FCC Rcd. 7123 (EB 2004) (revoking amateur operator's license after conviction for murder); *Trans Video Communications, Inc.*, 22 FCC Rcd. 855, ¶ 14 (WTB 2007) (revocation proceeding not warranted in the absence of any false statements in application or any willful or repeated rule violations after the grant of license).

[27] *See* 47 CFR § 2.939(c).

[28] Although Section 2.939(a)(4) authorizes the Commission to permit the withdrawal of an equipment authorization under other "conditions coming to the attention of the Commission," the identity and technical standard of Huawei's equipment, or parts thereto, have remained the same. Moreover, all withdrawals under Section 2.939(a) must be subject to the procedural safeguards based on an "appropriate rulemaking proceeding" and must "provide a suitable amortization period for equipment in hands of users and in the manufacturing process." 47 CFR § 2.939(c).

Furthermore, in making its decisions, the Commission must consider the whole record and address evidence contrary to its conclusions.[29] The Commission is required to explain "the evidence which is available" and "offer a rational connection between the facts found and the choice made."[30] Here, there is no rational basis for the Commission's proposal to deviate from the existing equipment authorization standards for a handful of disfavored companies. As Commissioner Starks has previously recognized, threats within 4G and legacy networks are primarily within the core network.[31] Prohibiting equipment authorizations to all Huawei RF equipment and devices, including inherently secure equipment (*i.e.*, equipment emitting low-level RF energy) that is not part of the core network, would not improve network security in any meaningful way.

C. Huawei's Equipment Has Been Recognized by Independent Third Parties, World Leading Carriers, Major Enterprise and Industry Customers as Being of the Highest Technical Quality.

The Commission cannot ignore the fact that Huawei's equipment is of the highest technical quality and has been subject to rigorous testing under the existing equipment authorization rules, all done by FCC-accredited testing laboratories. Since the launch of its operation in the United States in 2001, Huawei has gone to considerable effort to make sure that its equipment meets all

---

[29] *See, e.g.*, 5 U.S.C. § 556(d); *Allentown Mack Sales & Serv., Inc. v. NLRB*, 522 U.S. 359, 366 (1998); *AT&T Corp. v. FCC*, 86 F.3d 242, 247 (D.C. Cir. 1996) ("The substantiality of evidence must take into account whatever in the record fairly detracts from its weight.") (quoting *Universal Camera Corp. v. NLRB*, 340 U.S. 474, 488 (1951)). "[A]n agency cannot ignore evidence contradicting its position." *Butte County v. Hogen*, 613 F.3d 190, 194 (D.C. Cir. 2010).

[30] *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto Ins. Co.*, 463 U.S. 29, 52 (1983) (quotation marks omitted).

[31] *See* Commissioner Starks, Security Vulnerabilities within Our Communication Networks Workshop Report, at 10 (Nov. 21, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-360931A1.pdf ("At a high level the major components of a wireless network are the radio access network, or RAN, at the edge of the network, which consists of radios and antenna that communicate with individual handsets; . . . Workshop participants described the nature of threats within 4G and older networks as increasing as you move from the individual handsets to the RAN and on to the core").

Commission technical standards. In the last two decades, the Commission has not found any Huawei equipment falls short of those standards.

As one of the most advanced and praised manufacturers and service providers in the telecommunications industry, Huawei's equipment and devices are safe and secure. They have been subject to a robust testing and certification regime, evaluated and certified by multiple independent third-party certification bodies and labs. Huawei's equipment and devices have also passed the rigorous testing required by FCC-accredited TCBs. All Huawei products that have been imported to, marketed, and sold in the United States have been certified through the applicable FCC certification or SDoC procedures.

In addition to complying with RF emission rules, Huawei extensively cooperates with industry-recognized, FCC-accredited certification bodies and third-party labs to thoroughly test the cyber security and privacy protection capabilities of Huawei products, solutions, and services against industry standards and best practices. In 2020 alone, Huawei obtained more than 70 certifications worldwide related to cyber security and privacy protection.[32] Although cyber security and privacy are not currently among the criteria used in the FCC equipment authorization program, Huawei fully understands the critical importance of such factors and is confident that its products would comply with, if not exceed, any reasonable and objective standards that might be adopted in these areas.

To provide a uniform standard to guide its cybersecurity activities and risk management programs, Huawei devoted substantial resources to ensure its corporate governance and operation

[32] *Huawei 2020 Sustainability Report*, at 47 (2020), available at https://www-file.huawei.com/-/media/corp2020/pdf/sustainability/sustainability-report-2020-en.pdf.

structure comply with the most stringent certifications, including NIST CSF (cyber security framework), TISAX (information security and trusted information exchange in the automotive industry), ISO/IEC 27001 (information security management), ISO 28000 (security management for the supply chain), ISO/IEC 27017 (cloud security management), ISO/IEC 27018 (protection of personally identifiable information in public clouds), ISO/IEC 27701 (privacy information management), ISO/IEC 29151 (protection of personally identifiable information), CSA STAR (cloud security management), PCI DSS and PCI 3DS (payment card industry data security), SOC 1, 2, and 3 (system and organization controls), and ISO 27799 (health information security), to name a few.[33]

Moreover, Huawei has passed comprehensive audits, regular reviews, and stringent assessments conducted by many of the world's top carriers and major enterprise and industry customers on domains including cybersecurity and information security.[34] To further demonstrate Huawei's commitment to build a secure and trustworthy digital environment and to drive "Openness, Transparency and Collaboration," Huawei established Cyber Security Transparency Centers around the globe, in Britain, Brussels, Canada, China, Dubai, Germany, and Toronto, with the latest addition being a Global Cyber Security and Privacy Protection Transparency Center in Dongguan, China.[35]

Furthermore, Huawei has worked for years to ensure its equipment and devices align with industry best cybersecurity practices and compliance. These efforts continue to this day. The result is that Huawei's equipment, devices, and technologies have been recognized by its customers as

---

[33] *See Huawei 2020 Annual Report*, at 56 (2020), available at https://www-file.huawei.com/minisite/media/annual_report/annual_report_2020_en.pdf ("Huawei 2020 Annual Report").

[34] *Huawei 2020 Annual Report*, at 58.

[35] *See Huawei Cyber Security Transparency Centre*, available at https://www.huawei.com/us/trust-center/transparency; *see also Huawei Opens Its Largest Global Cyber Security and Privacy Protection Transparency Center in China* (Jun. 9, 2021), available at https://www.huawei.com/en/news/2021/6/huawei-largest-global-cyber-security-privacy-protection-transparency-center.

having the highest technical quality. In related proceedings, Huawei's customers, business partners, industry associations, and trade associations have already commented and dispelled the unfounded allegations against the security and quality of Huawei equipment:

- The Competitive Carriers Association commented that the Commission has identified "no specific evidence that Huawei … equipment and services create cybersecurity risk."[36]
- The head of Viaero Wieless ("Viaero") submitted a declaration that Viaero buys equipment and services from Huawei yet remains protected "from any malicious act."[37]
- The CEO of United Telephone Associations, Inc. ("United") likewise submitted a declaration that, even though "nobody wants to protect our National Security more than United," United feels comfortable using Huawei equipment. [38]
- NTCA—Rural Broadband adds that "border patrol agents … roam freely between U.S. network providers and those operated by neighboring countries which often rely upon Huawei equipment"—all without raising any apparent security concerns.[39]

---

[36] *See* Comments of Competitive Carriers Association, WC Docket No. 18-89, at 39-40 (filed Jun. 1, 2018) ("CCA Comments").

[37] *Id.*, DiRico Decl. ¶ 3.

[38] *Id.*, Houseman Decl. ¶ 6.

[39] Comments of NTCA—Rural Broadband, WC Docket No. 18-89, at 16 (filed Jun. 1, 2018).

- Mark Twain Communications Company, which uses "equipment manufactured by Huawei," has not seen any evidence that the blacklisting of the company is "even reasonably related … [to] the goal of national security."[40]
- Sagebrush Cellular, Inc. "has spent extensive time trying to find one shred of evidence that demonstrates any wrongdoing by Huawei and, to date, has been unable to uncover any hard fact."[41]

Huawei has also supported industry efforts to build a reliance ecosystem. For example, to support the Global Reporting Initiative and self-examine Huawei's sustainability performance, every year since 2008, Huawei has worked with a leading assurance provider to issue an annual sustainability report and disclose Huawei's sustainability performance assurance statement to facilitate communication, awareness, and interaction with its stakeholders.[42] Huawei's 2020 Sustainability Report specifically recognized the challenges and changes imposed by the COVID-19 pandemic and announced Huawei's commitment to developing secure and trustworthy digital products and services according to the highest cybersecurity and privacy protection standards.[43]

Huawei's equipment and devices have been recognized by independent third parties, leading telecommunication carriers, enterprise and industry customers as being of the highest technical quality and the Commission cannot simply ignore the substantial evidence demonstrating the attention that Huawei gives to ensuring the security of its products, services, and supply chain.

---

[40] Comments of Twain Communications, WC Docket No. 18-89, at 3-4 (filed Jun. 1, 2018).

[41] Comments of Sagebrush, WC Docket No. 18-89, at 4 (filed Jun. 1, 2018).

[42] *Huawei Sustainability Report from 2008 to 2020*, available at https://www.huawei.com/us/sustainability/sustainability-report.

[43] *See generally* 2020 Huawei Sustainability Report (2020).

D. The Commission's Proposal Cannot Be Justified by a Cost-Benefit Analysis.

The Commission seeks comment on the cost-effectiveness of the proposed rules.[44] The Commission's prohibition and revocation proposal is not and cannot be supported by a cost-benefit analysis.

In the NPRM, the Commission has not quantified and cannot quantify or document any benefits of revoking existing equipment authorizations of RF equipment. The Commission's continuing erroneous focus on the corporate origin and identity of equipment, rather than its security and technical specifications, overlooks the complexity of the global supply chain, where all vendors regardless of origin likely will include at least some Chinese-manufactured or produced components in their equipment. Even assuming (contrary to the evidence) that the proposed rules would remove *some* potentially risky equipment from the U.S. marketplace, much other equipment with components originating in China or other suspect countries will remain widely available in this country, and the overall risk to the U.S. public would be only minimally reduced. Moreover, there is no guarantee that any such equipment would be subject to the stringent cybersecurity and privacy standards that Huawei follows.

By contrast, the costs of the Commission's reliance on blacklists and bans are substantial and well-documented. The proposed rules will continue and expand the separation of the United States supply chain from China, resulting in harm to the leadership of United States companies by forcing them to shrink revenues and cut spending on research and development. In particular, the Commission should carefully consider all costs associated with revoking the existing equipment authorizations and the potential unforeseen impact on the supply chain. Even the U.S. govern-

[44] NPRM, ¶¶ 70-72.

ment's own National Intelligence Council has warned that splitting the world into several economic and security blocs will impose extraordinary costs, including "massive financial losses for countries and corporations, as supply chains fracture, markets are lost, and once lucrative sectors, like travel and tourism, decline."[45]

The proposed rules in this docket would also impair the potential benefits to U.S. consumers sought by other Commission proceedings. For example, on June 17, 2021, the Commission adopted targeted enhancements designed to modernize its marketing and importation rules to allow the early adoption of new technologies and permit U.S. consumer access to such devices.[46] The Earlier Opportunities Order modified the equipment authorization rules to incentivize and encourage more equipment manufacturers to produce "innovative products and [allow] consumers [to] benefit by seeing new products and features rolled out in a much shorter timeframe."[47] The proposed rules here will not only deprive U.S. consumers of early access to the latest products and innovations developed by Huawei, and hence damage U.S. global competitiveness and economic growth, but also discourage other similarly-situated equipment manufacturers from leveraging the new rules promulgated under the Earlier Opportunities Order, as the launch of any new products, even in light of the compressed development cycle, will be rendered useless should any company's products become subject to the Covered List.

More importantly, revoking existing equipment authorizations previously issued to Huawei equipment would impose disproportionate costs – in the hundreds of millions of dollars – on end-users, distributors, suppliers, and resellers of Huawei equipment, as existing users of Huawei

---

[45] *National Intelligence Council's Global Trends report*, 7th Edition (March 2021), available at https://www.dni.gov/index.php/gt2040-home/introduction.

[46] *Allowing Earlier Equipment Marketing and Importation Opportunities*, Report and Order, ET Docket No. 20-382, FCC 21-72 (rel. June 17, 2021) ("*Earlier Opportunities Order*").

[47] *Earlier Opportunities Order*, ¶ 4.

equipment will face significant difficulties and increased costs in obtaining replacement equipment, parts, or services. Requiring these United States entities to undertake redundant, unnecessary, and unlawful replacement efforts diverts limited resources, threatens service quality, and increases the cost of service.

Additionally, revoking existing authorizations would undermine multi-year contracts, including service agreements and contracts with voluntary extensions pertaining to the purchase and maintenance of covered equipment. As a result, the contracting parties would have to cancel purchase orders, stop paying for equipment already provided, suspend project and contract negotiations, and seek a reasonable replacement for existing equipment that can pass the Commission's equipment authorization rules. Even preventing Huawei from obtaining authorizations prospectively would harm U.S. businesses and consumers. It would eliminate resellers' ability to obtain, service, replace, and upgrade Huawei-made RF equipment in the future, including upgraded versions of RF equipment already in inventory and equipment already sold to customers. These high costs cannot be justified by the unspecified national security benefits, if any, of the proposed rules, which are wholly speculative. For these reasons, adopting the Commission's proposed rules notwithstanding the unintended consequences and foreseeable economic harm will only be an arbitrary and capricious action and clearly provide no cost benefit.[48]

[48] *See Nat'l Ass'n of Indep. Television Producers & Distributors v. FCC*, 502 F.2d 249, 255 (2d Cir. 1974) (invalidating a rule as imposing unreasonable secondary retroactivity where "petitioners had good reason to rely on their status under the [old] rule" and that "any effective date earlier than September 1975 would be unreasonable because it would cause serious economic harm to independent producers and because it gives networks inadequate time to plan additional programming").

Far more effective means exist to enhance security, such as prohibiting equipment that fails to satisfy specified design and technical standards, independent security testing, and/or other protocols and frameworks necessary to ensure national and network security, as explained in Section V below. These are the alternative means on which the Commission should focus.

III. THE COMMISSION LACKS STATUTORY AUTHORITY TO ADOPT THE PROPOSED RULES.

The Commission proposes adopting rules to prohibit equipment authorizations to communications equipment on the Covered List.[49] The Commission argues that its proposal is supported by relying on (1) the existing equipment authorization process to implement the Commission's "other statutory duties," (2) "other authorities" in the Communications Act of 1934, (3) "a potential alternative basis" under the Communications Assistance for Law Enforcement Act ("CALEA"), and (4) ancillary authority under the Secure Networks Act.[50]

None of these support the Commission's position. The Commission has not identified and cannot identify any explicit source of authority to implement a categorical ban under the established equipment authorization procedures to restrict further equipment authorization and the importation and marketing of Covered List equipment. Congress simply has not granted the Commission the authority to impose a blanket prohibition on the use of equipment on the Covered List. The Commission "literally has no power to act unless and until Congress confers power upon it."[51] Absent any rulemaking authority under existing statutes, the Commission cannot lawfully propose revisions to existing equipment authorization rules to ban all equipment authorization.

---

[49] NPRM, ¶ 41.

[50] NPRM, ¶¶ 65-69 (citing Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (the "Secure Networks Act")).

[51] *Mozilla Corp. v. FCC*, 940 F.3d 1, 74 (D.C. Cir. 2019) (per curiam) (internal citations omitted); *accord Collins v. Mnuchin*, 938 F.3d 553, 562 (5th Cir. 2019) (en banc); *see* 5 U.S.C. § 706(2)(C).

A. The Proposed Rules Exceed the Commission's Authority to Impose Technical Equipment Standards.

The Commission argues that its statutory authority to regulate RF equipment can serve the purpose of fulfilling the Commission's responsibilities under the Secure Networks Act and "other statutory duties."[52] As explained further below, the Commission's equipment authorization rules were adopted pursuant to express statutory provisions that deal with technical issues, and none authorize the Commission to prohibit the importation, marketing, or sale of a company's products *en masse* without regard to the technical characteristics of a particular product (with one exception specifically required by statute and premised on a prior criminal conviction of the registrant).

To begin with, the NPRM itself recognizes that the purpose of the equipment authorization rules is "to promote efficient use of the radio spectrum."[53] Indeed, the specific rule cited by the Commission expressly states that the rules are focused on technical criteria.[54] And it is the Chief of the Office of Engineering and Technology, a technical advisor to the Commission, who is charged with administering the equipment authorization program by conducting engineering and technical analysis, testing equipment to determine its interference risks and operating parameters, and developing projects to gather theoretical and experimental data on new technologies.[55] Based

---

[52] *Id.* (citing 47 CFR §§ 2.901, 2.1091-.1093, 2.925(b)(2), 2.1033(d), & 1.2002(a)).

[53] NPRM, ¶ 65 (citing 47 CFR § 2.901 and 47 U.S.C. § 303(g)); *see also* NPRM, ¶ 23.

[54] 47 CFR § 2.901 ("In order to carry out its responsibilities under the Communications Act and the various treaties and international regulations, and in order to promote efficient use of the radio spectrum, the Commission has developed *technical standards* for radio frequency equipment and parts or components thereof. The *technical standards* applicable to individual types of equipment are found in that part of the rules governing the service wherein the equipment is to be operated. In addition to the technical standards provided, the rules governing the service may require that such equipment be authorized under Supplier's Declaration of Conformity or receive a grant of certification from a Telecommunication Certification Body.") (emphasis added).

[55] *See* 47 C.F.R. § 0.241(b).

upon the established technical standards, the Commission recognizes that certain RF devices subject to the NPRM "generate such low levels of RF emission that they have virtually no potential for causing harmful interference to [t]he authorized radio services."[56] Under the proposed rule, however, the Commission would prohibit all RF devices of targeted manufacturers from receiving an equipment authorization, even those devices with "virtually no potential" for "harmful interference[.]" This would be arbitrary and capricious, and therefore unlawful.

The NPRM argues that Section 302 alone is not the only authority for equipment regulations, since the equipment authorization rules "address other policy objectives – such as human RF exposure limits, hearing aid compatibility with mobile handsets, and the Anti-Drug Abuse Act of 1988."[57] It is true that these rules include provisions that implement more than one statutory directive. However, each of these "other policy objectives" is derived from explicit statutory authority that directed the Commission to adopt the additional requirements, not from Commission decisions to include extraneous provisions in the rules on vague policy grounds.

First, the Commission's rules regulating human RF exposure are authorized by the National Environmental Policy Act ("NEPA").[58] Pursuant to the NEPA, the Commission took a number of steps "to evaluate the effects of our actions on the quality of the human environment, including human exposure to RF energy emitted by Commission-regulated transmitters and facilities."[59] *Second*, the Commission's rules relating to hearing aid compatibility are authorized by

---

[56] NPRM, ¶ 31.

[57] NPRM, ¶ 23.

[58] NPRM, ¶ 65 (citing 47 CFR §§ 2.1091-.1093).

[59] *See Proposed Changes in the Commission's Rules Regarding Human Exposure to Radiofrequency Electromagnetic Fields, et al.*, Resolution of Notice of Inquiry, Second Report and Order, Notice of Proposed Rulemaking, and Memorandum Opinion and Order, 34 FCC Rcd 11687, 11688, ¶ 1 (2019).

Section 710 of the Communications Act,[60] which expressly requires the Commission to "ensure reasonable access to telephone service by persons with impaired hearing" and to implement regulations governing "customer premises equipment."[61] *Third*, the Anti-Drug Abuse Act of 1988 ("ADAA") requires the Commission "to deny federal benefits to certain individuals who have been convicted multiple times of federal offenses related to trafficking in or possession of controlled substances."[62] The ADAA also requires any entity receiving a "federal benefit" to certify compliance with ADAA requirements.[63] The Commission accordingly found that a wide range of Commission-regulated entities in various services must certify compliance with ADAA requirements.[64]

Here, in contrast, neither Section 302 nor 303 of the Communications Act explicitly grants the Commission any authority to adopt additional requirements to treat *all* equipment on the Covered List, without regard to the technical parameters of any particular item, as a threat to the national security.[65] Nor does any other statute, including the Secure Networks Act, specifically require or authorize the Commission to adopt a categorical ban on authorization of RF devices based on the Covered List. And, apart from the specific requirement of the ADAA, no statute allows the Commission to grant or withhold equipment authorizations based solely on the identity of the manufacturer.

---

60 *See* NPRM, ¶ 65 (citing 47 CFR §§ 2.925(b)(2), 2.1033(d) & 47 U.S.C. § 610).

61 *See* 47 U.S.C. §§ 610(a), (b).

62 NPRM, ¶ 65.

63 *Id.*

64 *See* 47 CFR § 2.911(d)(2) (requiring a certification that the applicant is not subject to a denial of Federal Benefits pursuant to the ADAA); *Amendment of Part 1 of the Commission's Rules to Implement Section 5301 of the Anti-Drug Abuse Act of 1988*, Gen. Docket No. 90-312, Report and Order, 6 FCC Rcd 7551 (1991) ("ADAA Report and Order"); For example, the Commission requires all requests for Special Temporary Authority and other non-application-form (*e.g.*, letter) to include an ADAA certification, affirming that the applicant is not subject to a denial of federal benefits that includes the Commission benefits under the ADAA.

65 *See* 47 U.S.C. §§ 302a, 303.

B. No Statute Explicitly Gives the FCC Any Discretion to Withhold or Revoke Equipment Authorizations Based on National Security Considerations Regardless of the Equipment's Compliance with Technical Standards.

While the Commission admitted that the proposed rules are "not specifically authorized by the Secure Networks Act itself, pursuant to which the Commission adopted the Covered List," it nevertheless argues that it has broad authority to adopt the proposed rules to implement other statutory duties authorized by a handful of other statutory provisions.[66] But none of these authorities confers on the Commission the authority to engraft a general prohibition for certain equipment on its existing equipment authorization rules. It is a fundamental rule that agencies may not take action "in excess of statutory jurisdiction, authority, or limitations."[67] Yet, that is precisely what the Commission is proposing to do in this case.

1. Section 302 of the Communications Act Cannot Provide the Authority.

The Commission asserts that Section 302 of the Communications Act of 1934,[68] as amended, provided it with sufficient legal authority underpinning the proposed rules.[69] Specifically, the Commission refers to language in Section 302(a) that authorizes the Commission to "consistent with the public interest, convenience, and necessity, make reasonable regulations."[70] The Commission adds that Section 302(a) authorizes the Commission to promulgate rules "applicable to the manufacture, import, sale, offer for sale, or shipment of such devices and … to the use

---

[66] NPRM, ¶¶ 65-67 (citing 47 U.S.C. §§ 302a(a), 303(e), 303(g); 42 U.S.C. § 4321 *et seq*; 21 U.S.C. § 862).

[67] 5 U.S.C. § 706(2)(C).

[68] 47 U.S.C. § 302a.

[69] NPRM, ¶ 65 (citing 47 U.S.C. § 302a).

[70] *Id.* (quoting 47 U.S.C. § 302a(a)(1)).

of such devices."[71] However, it plucks these phrases out of their context in the statute, and therefore distorts their meaning and intent.

Section 302 only authorizes the Commission to make reasonable regulations (1) "governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications" and (2) "establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy."[72] References to the "public interest" and to "reasonable regulations" in that Section must be addressed to these two specifically stated purposes. In fact, the Commission itself recognized that the authorization processes are primarily for the purpose of evaluating equipment's compliance with technical specifications intended to minimize the interference potential of devices that emit RF energy.[73]

Despite the Commission's contrary assertions, Section 302(a) does not authorize the Commission to make regulations restricting equipment and devices based on criteria other than RF emissions and interference, such as the identity of the manufacturer and speculative national security concerns. Principles of statutory interpretation require that when a statute explicitly identifies a set of requirements to be followed by an agency, the agency lacks discretion to rely on alternative grounds to justify its actions.[74]

---

[71] *Id.* (quoting 47 U.S.C. § 302a(a)(2)).

[72] 47 U.S.C. § 302a(a).

[73] NPRM, ¶ 65.

[74] *See, e.g., Jennings v. Rodriguez*, 138 S. Ct. 830, 844 (2018) ("[T]he expression of one thing implies the exclusion of others."); *Gibbons v. Ogden*, 9 Wheat. 1, 195 (1824) (Marshall, C.J.) ("The enumeration presupposes something not enumerated.").

References to technical capability, not the identity of the manufacturer, elsewhere in Section 302 also confirm that the Commission does not have authority to base regulations on non-technical considerations. Section 302(d), for example, provides that the Commission shall deny equipment authorization for any scanning receiver that is capable of: (1) "receiving transmissions in the frequencies allocated to the domestic cellular radio telecommunications service," (2) "readily being altered by the user to receive transmissions in such frequencies," or (3) "being equipped with decoders that convert digital cellular transmissions to analog voice audio."[75] The identity of the manufacturer is not part of the inquiry prescribed by the statute; the technical capability of the equipment is.

The Commission further proposes to rely on the "public interest" phrase in Section 302 to provide independent authority to ban equipment authorization.[76] The "public interest" phrase in Section 302 does not and cannot provide such independent authority for at least two reasons.

First, the reference to the public interest in the context of Section 302 clearly refers to the interference potential of devices, not the identity of a manufacturer. Section 302 applies only to "devices which interfere with radio reception," and even the broadest definition does not encompass *all* equipment or services produced or provided by a company.[77] Yet the proposed rules would apply to all RF equipment and devices specified on the Covered List irrespective of whether the device is "capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications."[78]

---

[75] 47 U.S.C. § 302a(d).

[76] NPRM, ¶ 66.

[77] 47 U.S.C. § 302a.

[78] 47 U.S.C. § 302a(a).

Second, the Commission's interpretation contradicts the Supreme Court, which has consistently recognized that a statutory reference to "the public interest" in the Communications Act "is to be interpreted by its context" and "is not to be interpreted as setting up a standard so indefinite as to confer an unlimited power."[79] Accordingly, when the Commission issues rules, those rules must rest on specific grants of authority as defined by the relevant section of the Communications Act—not on an open-ended "public interest" authorization to consider any policy considerations the agency chooses, regardless of its statutory charter or area of expertise.

2. Section 303 of the Communications Act Also Does Not Authorize the Commission's Proposed Rules.

Nor are the proposed rules within the Commission's "other statutory responsibilities" under the Communications Act, including under Sections 303(e) and 303(g).[80] Section 303(e) of the Communications Act states that the Commission may "[r]egulate the kind of apparatus to be used [by radio licensees] with respect to its *external effects* and the purity and sharpness of the emissions from each station and from the apparatus therein."[81] In the context of the statute, the mention of the words "external effects" makes clear that Section 303 only refers to equipment used by licensed operators of radio transmitters in radio stations and the external effects of their RF emissions, not some other unrelated types of effects. The other subsections also make it abundantly clear that Section 303 is intended to prevent interference between stations, and the proposed rules would do

---

[79] *See Nat'l Broad. Co. v. United States*, 319 U.S. 190, 216 (1943) ("The 'public interest' to be served under the Communications Act is … the interest of the listening public in 'the larger and more effective use of radio.'"); *see also e.g.*, *NAACP v. FPC*, 425 U.S. 662, 669 (1976) ("This Court's cases have consistently held that the use of the words 'public interest' in a regulatory statute is not a broad license to promote the general public welfare.").

[80] NPRM, ¶ 65.

[81] 47 U.S.C. § 303 (emphasis added).

nothing to accomplish that purpose.[82] In addition, Section 303 exempts many specific types of equipment, such as display-only video monitors with no playback capability[83] and navigation devices,[84] whereas the proposed rules include no exemptions and are based solely on the manufacturer's identity. Accordingly, the Commission's unbounded view of its authority under Section 303 is an unreasonable and impermissible expansion of the scope and reach of "the kind of apparatus" Section 303(e) intends to cover.

While Section 303(g) of the Communication Act requires the Commission to "generally encourage the larger and more effective use of radio in the public interest,"[85] this provision does not salvage the Commission's lack of authority either. Apart from a general reference to Section 303(g) to support the notion that the Commission must "promote efficient use of the radio spectrum," the NPRM points to no authority for the Commission to prohibit the issuance of equipment authorization.[86] Indeed, there is no rational basis for asserting that the removal of Huawei equipment from the United States would "encourage the larger and more effective use of radio" at all. Furthermore, just as with Section 302, the Commission cannot rest on the term "public interest" and use Section 303(g) as an independent authority for the proposed rules.

---

[82] *See, e.g.*, 47 U.S.C. § 303(a) (classifying "radio stations"); *id.* § 303(b) (prescribing "class of licensed stations"); *id.* § 303(c) (assigning "banks of frequencies"); *id.* § 303(d) (determining the location of "stations"); *id.* § 303(g) ("prevent interference between stations"); *id.* § 303(h) ("establish areas or zones to be served by any station"); *id.* § 303(i) (authorizing to make general rules and regulations relating to "stations"); *id.* § 303(j) (make general rules and regulations relating to "stations"); *id.* § 303(k) (exclude certain "radio stations").

[83] 47 U.S.C. § 303(u)(2)(B).

[84] 47 U.S.C. § 303(aa)(4).

[85] 47 U.S.C. § 303(g).

[86] NPRM, ¶ 65.

3. The Communications Assistance for Law Enforcement Act Can Not Provide A Source of Authority.

Continuing its search for authority to support its proposed action, the Commission asks whether the Communications Assistance for Law Enforcement Act ("CALEA") could provide an alternative source of authority for the proposed rules.[87] Specifically, the Commission cites Section 105 of CALEA (47 U.S.C. § 1004) as possible authority for the proposed rules and seeks comment on whether the proposed rules can be justified as an implementation of CALEA. As Huawei explained in prior related filings, the Commission lacks the power to authorize a ban or remove and replace covered equipment under CALEA.[88] Similarly, the proposed rules in this proceeding cannot be authorized based on CALEA for at least the following reasons.

First, the plain language of CALEA does not address equipment authorization or authorize the FCC to ban broad categories of equipment. Rather, Section 1004 provides as follows:

> A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information *effected within its switching premises* can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.[89]

In the NPRM, the Commission acknowledged that the security requirements of CALEA "apply directly to equipment intended for use by providers of telecommunications services."[90] The Commission nonetheless claims that it can interpret Section 1004 to "prohibit[] the use of equip-

---

87 NPRM, ¶ 68 (citing 47 U.S.C. §§ 1001-1010).

88 *See, e.g.*, Comments of Huawei, WC Docket No. 18-89, at 26-27 (filed Aug. 3, 2020); Reply Comments of Huawei, WC Docket No. 18-89, at 4-5 (filed Mar. 3, 2020); Comments of Huawei, WC Docket No. 18-89, at 18-19 (filed Feb. 3, 2020); Written *Ex Parte* of Huawei, WC Docket No. 18-89, at 2-16 (filed Nov. 14, 2019).

89 47 U.S.C. § 1004.

90 NPRM, ¶ 68.

ment produced or provided by any company posing a national security threat," by anyone anywhere, as if the terms "telecommunications carrier" and "effected within its switching premises" were not in the statute.[91] The cardinal rule of statutory interpretation is "that a legislature says in a statute what it means and means in a statute what it says there."[92] "[E]very clause and word of a statute" must be given effect, and "if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant."[93] Consequently, when Section 1004 states that it applies to communications interceptions "effected within [a carrier's] switching premises,"[94] that is exactly what the statute means – the statute covers communications interceptions only when they are effected within a carrier's switching premises. It cannot possibly authorize the Commission to regulate equipment without regard to whether it is used by a carrier, used within switching premises, or even capable of being used to intercept anything. The Commission's proposed rules are outside of the scope of Section 1004 and its attempt to find legal justification in that provision is irrationally broad.

Second, Congress enacted CALEA to require telecommunications carriers to make tools available to "enabl[e] the *government*" to intercept communications "pursuant to a court order or other lawful authorization."[95] That is precisely why Section 1004 does not reach beyond a carrier's "switching premises" and why it requires "the affirmative intervention of an individual officer or

---

91 *Id.*

92 *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992).

93 *Duncan v. Walker*, 533 U.S. 167, 174 (2001) (citations omitted).

94 47 U.S.C. § 1004.

95 47 U.S.C. § 1002(a) (emphasis added) (listing the four interception capabilities required by the government); *see also id.* § 1001(5) ("The term 'government' means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance.").

employee of the carrier." The statute does not impose any requirement of interception capabilities on a carrier beyond its switching premises. Correspondingly, it does not impose any requirements for preventing interception beyond the carrier's switching premises.[96] The Commissions' proposal attempts to prohibit all future authorizations for equipment on the Covered List, regardless of whether the equipment is within a carrier's switching premises, and would require an impermissibly broad and unintended interpretation of CALEA that would be arbitrary and capricious, and contrary to law.

Third, the legislative history of CALEA likewise clarifies that the purpose of the statute is to impose a requirement on carriers to assist law enforcement and corresponding protections against law enforcement abuse. The focus of CALEA is signal interception on carriers' *switching premises*, while the Commission's existing equipment authorization process deals broadly with a wide variety of RF equipment and devices, not within that physical limitation. The legislative history further clarifies that the government agencies do not have the authority to intercept signals from any equipment and do not reach communications that do not occur on the carrier "switching premises."[97]

Fourth, the Commission's failure to interpret "switching premises" would result in absurd and undue consequences. By removing this limitation, CALEA would effectively require telecommunications carriers to ensure that no unauthorized interceptions can occur at any "point[] in [its] network where an interception might be activated." And if the Commission were to implement

---

[96] *See id.* § 1004.

[97] Compare H.R. Rep. 103-827, at 26 ("All executions of court orders or authorizations requiring access to the switching facilities will be made through individuals authorized and designated by the telecommunications carrier.") *with id.* ("Activation of interception orders or authorizations originating in local loop wiring or cabling can be effected by government personnel"—that is, not on carrier switching premises and not by carrier employees.).

CALEA's requirements under this interpretation, a carrier would be liable if it failed to prevent an unauthorized attempt to tamper with communications equipment at, for example, a consumer's premise.

Accordingly, CALEA's structure and legislative purpose make clear that the statute applies only to interception of communications by law enforcement or via tools created by carriers to permit interception of communications by law enforcement at the switching premises, and not to any other use of RF equipment for any purpose by any user at any place.

C. The Commission also lacks ancillary authority to promulgate the proposed rules.

The Commission tacitly acknowledges its lack of statutory authorization by seeking to rely on ancillary jurisdiction under Title I of the Communications Act.[98] The Commission asserts that it has ancillary authority under the broad language of Section 4(i) of the Communications Act to adopt the proposed rules as "reasonably necessary" to enforce the Secure Networks Act.[99] Despite the Commission's claim, the reach of the Commission's ancillary jurisdiction is not unbounded, and the proposed rules do not fall within that jurisdiction.

If there is a bedrock principle underlying the Commission's ancillary jurisdiction, it is that the Commission may exercise ancillary jurisdiction only when two conditions are satisfied: (1) when the subject of the regulation is within the general scope of the agency's expertise under Title I covering the regulated subject *and* (2) when the proposed regulation is reasonably ancillary to the effective enforcement of some specific statutorily mandated responsibilities.[100] The Com-

---

98 NPRM, ¶ 69.

99 *Id.*

100 *See American Library Ass'n v. FCC*, 406 F.3d 689, 691-92 (D.C. Cir. 2005).

mission cannot exercise ancillary authority based on a mere policy statement, as this would "contravene the axiomatic principle that administrative agencies may [act] only pursuant to authority delegated to them by Congress."[101]

The flaw in the Commission's claim of ancillary jurisdiction turns on one simple fact: the Secure Networks Act reflects a specific and narrow Congressional intent to prohibit the direct or indirect use of specific Federal subsidies through a program administered by the Commission to purchase covered equipment or services used by providers of advanced communications service. It does not give the Commission general jurisdiction to regulate any other use of covered equipment or services. The plain text of the Secure Networks Act confirms that Congress did not intend to confer "unbounded" jurisdiction on the Commission.

To begin with, Section 2 of the Secure Networks Act requires the Commission to publish and maintain a list of "covered communications equipment or services" that could undermine the security of U.S. networks.[102] The Covered List explicitly does not encompass *all* communications equipment or services, and inclusion on the list is not based on anything related to RF emissions. Instead, to be included, equipment and services must be "communications equipment or service," based on a technical determination, "if and only if such equipment or service" is capable of:

> (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.[103]

---

[101] *Verizon v. FCC*, 740 F.3d 623, 632 (D.C. Cir. 2014) (quoting *American Library Ass'n*, 406 F.3d at 691) (quotation marks omitted).

[102] 47 U.S.C. § 1601.

[103] 47 U.S.C. § 1601(b)(2).

The Commission itself has interpreted this definition under Section 2 to include equipment capable of "causing an advanced communications service provider's network to be remotely disrupted, or otherwise posing an unacceptable risk to United States national security" and noted that it does not reach end-user equipment.[104]

Any further uncertainty is dispelled by the Secure Networks Act itself, which defines "communications equipment or service" as "any equipment or service that is essential to the provision of advanced communications service."[105] The Commission has consistently interpreted the term "advanced communications service" to include "all equipment or services used in fixed and mobile broadband networks, provided they include or use electronic components"[106] and "services with any connection of at least 200 kbps in any direction."[107] The Commission's proposed rules are not limited to this type of equipment, and therefore cannot be justified as ancillary to the Secure Networks Act.

Furthermore, Section 4 of the Secure Networks Act establishes a purely voluntary Secure and Trusted Communications Networks Reimbursement Program ("Reimbursement Program") based on the Covered List. Again, the Congressional mandate is that only eligible participants may receive reimbursement under this program. At the outset, the Reimbursement Program is only available to carriers providing advanced communications services who choose to remove, replace,

---

[104] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Second Report and Order, WC Docket No. 18-89, 35 FCC Rcd 14284, 14300, fn. 103 (rel. Dec. 11, 2020) (citing Secure Networks Act § 2(b)(2)(A)-(C)) ("*Second Report and Order*").

[105] "Communications equipment or service" means "any equipment or service that is essential to the provision of advanced communications service." Secure Networks Act § 9(4)).

[106] *Second Report and Order*, ¶ 53.

[107] *Second Report and Order*, ¶ 55 (noting that no commenter opposed this definition); *see also Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 35 FCC Rcd 7821, 7829, ¶ 27 (2020).

and dispose of equipment and services identified on the list.[108] In fact, not all carriers providing advanced communications services are eligible, as participation in the Reimbursement Program is limited to providers of a specific size and type.[109]

Additionally, the Secure Networks Act prohibits using a Federal subsidy available through a program administered by the Commission to (1) purchase, rent, lease, or otherwise obtain any covered communications equipment or service; or (2) maintain any covered communications equipment or service previously purchased, rented, leased, or otherwise obtained.[110] No provision of the Secure Networks Act (including Section 4) supports denial of equipment authorization to covered equipment.

These provisions are an insufficient foundation for the Commission's effort to exercise its ancillary jurisdiction here because the Commission's proposed rules are designed to address entirely different circumstances. When Congress passed and the President signed into law the Secure Networks Act in 2020, it did so against the backdrop of using certain Federal loans, grants, and subsidies to purchase specific advanced communications equipment or services on the Covered List.[111] Here, by contrast, the proposed rules do not concern any Federal subsidy or funding. The Secure Networks Act also contains specific reporting and violation mechanisms,[112] and it is thus

---

[108] 47 U.S.C. § 1603(b).

[109] 47 U.S.C. § 1603(b)(1).

[110] 47 U.S.C. § 1602.

[111] *See, e.g.*, 20204998, CRS Summary, 116th Congress (2019-2020) (describing the Secure Networks Act as a bill to "prohibit[] the use of certain federal funds to obtain [covered] communications equipment or services").

[112] Section 5 of the Secure Networks Act establishes a reporting requirement whereby providers of advanced communications service must report whether the provider has purchased, rented, leased, or otherwise obtained any covered communications equipment or service; Section 7 prescribes the penalties for violations of the Secure Networks Act.

unnecessary and duplicative for the Commission to take additional action that would not accomplish the Secure Network Act's goals of restricting the use of Federal subsidies and Reimbursement Program funding.

Accordingly, the Commission's proposed rules are not reasonably ancillary to the effective enforcement of the Reimbursement Program, as the plain text of the Secure Networks Act and certain aspects of the statutory structure all indicate that the Secure Networks Act was not enacted to categorically bar the equipment authorization of all equipment on the Covered List.

IV. THE PROPOSED RULES ARE UNCONSTITUTIONAL AND VIOLATE THE ADMINISTRATIVE PROCEDURE ACT.

The Commission asks whether it should take steps to revoke existing equipment authorizations of "covered" communications equipment and seeks to identify the processes for doing so.[113] Even if the Commission has authority to do so, which it does not, the proposed revocation mandate will result in due process violations and unlawful primary and secondary retroactivity.

A. Revocation of Existing Authorizations Would Constitute Regulatory Taking of Property Interests Without Due Process Protection.

Huawei's existing equipment authorizations are property rights protected by the U.S. Constitution. The proposed rules, if adopted, would violate Huawei's Due Process rights by depriving the company of its constitutionally protected property.

Due process is "the protection of the individual against arbitrary action"[114] and the Constitution requires "that the government take reasonable measures to ensure basic fairness to the private party and that the government follow procedures reasonably designed to protect against

[113] NPRM, ¶¶ 80-89.

[114] *Ohio Bell Tel. Co. v. Pub. Utils. Comm'n of Ohio*, 301 U.S. 292, 302 (1937).

erroneous deprivation of the private party's interests."[115] Under the Due Process Clause, the Commission may not revoke Huawei's property interests unless it first provides the company with notice and the opportunity for a meaningful individualized hearing on the charges against it, even if the Commission has the authority to revoke the equipment authorizations, which it does not.[116] Such a hearing must include a "notice of the factual basis" for a material government finding and "a fair opportunity to rebut the Government's factual assertions before a neutral decision-maker" to avoid "erroneous deprivation."[117] Further, the hearing must, at a minimum, constitute a formal adjudication that complies with the APA's rigorous "on the record" hearing requirements. These most critical procedural protections are totally missing here.

The proposed rules and revocation mandate fail to provide even the minimal procedural protections to affected equipment and manufacturers. There is no notice, no hearing procedure, no opportunity to review evidence, and no opportunity to respond to evidence. Using rulemaking as a disguise, the Commission's approach would single out a small group of companies by tying the existing equipment authorization procedure designed for RF equipment with the Covered List, notwithstanding the fact that the Covered List was created based on an entirely separate rule intended to prohibit carriers from using Commission subsidies to purchase equipment and services identified on the Covered List. Effectively, by revoking existing equipment authorizations solely because such equipment is on the Covered List, the Commission is treating that Covered List as an "automatic" substitute for a meaningful hearing, and thereby depriving Huawei of the procedural protections required by the Constitution.

---

[115] *Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965, 980 (9th Cir. 2012).

[116] *Wolff v. McDonnell*, 418 U.S. 539, 557–58 (1974).

[117] *Kirk v. Comm'r of Soc. Sec. Admin.*, No. 19-1989, 2021 WL 387022, at *8 (4th Cir., Feb. 4, 2021).

B. The Proposed Rules Would Violate the Bill of Attainder Clause by Singling Out Huawei For Punishment.

Relatedly, the proposed rules would constitute an unlawful bill of attainder. The Bill of Attainder Clause of the Constitution states: "No Bill of Attainder or ex post facto Law shall be passed."[118] The Constitution does not define "bill of attainder," but according to the Supreme Court, a bill of attainder is "a legislative act which inflicts punishment without a judicial trial."[119] The proposed rules, if adopted, would single out Huawei by effectively precluding all Huawei RF equipment from being imported, marketed, and used in the United States, even if such equipment is not connected to any communications network, as prescribed by the Covered List. Yet, there is absolutely no logical nexus between the Covered List and the proposed rules. The proposed rules thus are based on and motivated by a blatant intent to inflict "punishment" without a hearing by subjecting Huawei to permanent and inescapable burdens solely and exclusively on the basis of its identity, instead of the technical standards prescribed by the existing equipment authorization rules to be neutrally applied by Commission and the TCBs. In doing so, the proposed rules amount to an unconstitutional bill of attainder.

C. The Proposed Rules Would Violate the Administrative Procedure Act by Imposing Primary Retroactivity and Unreasonable Secondary Retroactivity.

Rules permitting revocation of an authorization for equipment that complied with the rules in effect at the time it was authorized would additionally violate the APA by imposing primary retroactivity and unreasonable secondary retroactivity. A rule imposes primary retroactivity and is invalid under the APA if it "takes away or impairs vested rights acquired under existing laws, or creates a new obligation, imposes a new duty, or attaches a new disability, in respect to transactions

---

[118] U.S. Const. art. I, § 9, cl. 3.

[119] *United States v. Lovett*, 328 U.S. 303, 315 (1946).

or considerations already past," since the APA only authorizes rules that have "future effect."[120] A rule that alters the future legal consequences of past actions imposes secondary retroactivity, and a "rule that has unreasonable secondary retroactivity—for example altering future regulation in a manner that makes worthless substantial past investment incurred in reliance upon the prior rule—may for that reason be 'arbitrary' or 'capricious,' … and thus invalid" under the APA.[121] "A secondarily retroactive rule is valid only to the extent that it is reasonable—both in substance and in being made retroactive."[122] The proposed rules would impose both primary retroactivity and unreasonable secondary retroactivity—each providing an independent basis for invalidation under the APA.

The proposed rules would impose primary retroactivity because revocation of previously granted equipment authorizations would attach a "new disability" to past conduct. As discussed above, the existing equipment authorizations rules permit revocation of an authorization only if there is clear and convincing evidence of egregious misconduct by Huawei (*e.g.*, false statement or misrepresentation, nonconformity to technical requirements, unauthorized changes to the equipment).[123] Notwithstanding the fact that Huawei has always been able to supply certified and authorized equipment and services to carriers and customers, the proposed rules would allow for revocation of the authorizations of all Huawei RF equipment and render that equipment unmarketable in the U.S.

---

[120] *National Mining Ass'n v. DOL*, 292 F.3d 849, 859 (D.C. Cir. 2002); *Bowen v. Georgetown University Hosp.*, 488 U.S. 204, 218-19 (Scalia, J., concurring).

[121] *Bowen*, 488 U.S. at 219-220 (1988) (Scalia, J., concurring).

[122] *U.S. AirWaves, Inc. v. FCC*, 232 F.3d 227, 233 (D.C. Cir. 2000).

[123] Revocation would be reasonable if, hypothetically, it was based on misconduct that violated the rules *in effect* at the time of the violation. But the proposed rules go beyond that and also seek to revoke authorizations that were obtained in compliance with the rules that existed at the time they were issued.

The proposed rules also would impose unreasonable secondary retroactivity because they would adversely and unreasonably alter the legal consequences of past actions and undermine "reliance upon the pre-existing rule."[124] As drafted, the Commission's proposed rules would render covered RF equipment essentially useless and thus nullify any future benefit that users of Huawei RF equipment reasonably expected when they engaged in contractual transactions to purchase, supply, and use the covered RF equipment. Revoking the existing authorizations granted to that equipment based on non-technical criteria that did not exist at the time the authorizations were granted would "mak[e] worthless substantial past investment incurred in reliance upon the prior rule," and, therefore, be invalid under the APA.[125]

V. THE COMMISSION SHOULD LOOK TO EXISTING PROGRAMS AND FRAMEWORKS TO STRENGTHEN CYBERSECURITY.

In the NOI, the Commission proposes to leverage its equipment authorization program to encourage device manufacturers to consider cybersecurity standards and guidelines and incentivize better cybersecurity practices to build resilience and secure communications networks.[126] The Commission seeks comments on the form, structure, and standards the Commission should follow to establish a program to allow manufacturers to certify during the equipment authorization process.[127] The Commission also asks the extent to "other incentives or considerations that could encourage manufacturers to build security into their products."[128]

Huawei fully supports the Commission's goal of advancing and improving the security of RF communications. However, cybersecurity is a critical issue for *all* equipment in the telecom

---

[124] *Bowen* 488 U.S. at 219-20 (1988) (Scalia, J., concurring).

[125] *Id.* at 220.

[126] NPRM, ¶¶ 98-105.

[127] *Id.* at ¶ 102.

[128] *Id.*

network, not just that of a few specific manufacturers. Rather than blanket authorization bans on covered equipment, the Commission should promptly reinvigorate prior efforts to leverage voluntary means of securing networks and devices based on continued cooperation and participation of all stakeholders.

A. The U.S. Government, Expert Advisors to the Commission, and Industry Agree That a Risk-Management Approach to Security Is More Appropriate Than Categorical Bans on Certain Providers.

The global telecommunications supply chain is complex and dynamic, and security risks arise from the cumulative supply chain—not from the name that appears on the finished product. Security risks are not unique to Huawei's (or any other vendor's) equipment because of the global supply chain. All vendors, whether based in the U.S., China or elsewhere, likely include at least some Chinese-manufactured or produced components in their equipment and/or software. Continuing to focus on targeting a few specific suppliers, while ignoring the interdependent global supply chain on which virtually all equipment manufacturers and suppliers rely, would do little or nothing to address the real cybersecurity threat. As one security firm put it, the "exclusion of any single vendor or set of vendors from participating in U.S. carrier network contracts does little to address the actual risks" from a global supply chain.[129]

Policies and recommendations adopted by the U.S. government itself support this view. The National Institute of Standards and Technology ("NIST") has explained that "[s]upply chains

[129] Comments of RBA, WC Docket No. 18-89, Ex. 1, at 1 (filed Jun. 1, 2018) (citing Recommendations of Domain 5, FCC 18-42).

are complex, globally distributed, and interconnected sets of resources and processes between multiple levels of organizations."[130] As a result, information and communications-technology "products … or services originating anywhere (domestically or abroad) might contain vulnerabilities that can present opportunities for … supply chain compromises."[131] NIST's Cybersecurity Framework promotes a risk-management approach to cybersecurity and risk to the supply chain. In 2018, NIST released a revised version of its cybersecurity framework that provided further guidance on how organizations (including government agencies) should assess and manage cyber supply-chain risks.[132] The voluntary framework explains that steps to mitigate cyber supply-chain risks may include determining cybersecurity requirements for suppliers, enacting those requirements through mechanisms such as contracts, and verifying satisfaction of those requirements through various assessment methodologies such as audits and testing.

Additionally, in 2020, when drafting NIST's Internet of Things ("IoT") device cybersecurity core baseline, NISTIR 8259A, NIST promoted multi-stakeholder collaboration and recognized that adoption of cybersecurity capabilities should be voluntary and vary across different organizations' operating contexts and risk environments.[133] Even more recently, following a White House cybersecurity summit that involved corporate leaders and U.S. government officials, U.S. Secretary of Commerce Raimondo announced that NIST would "partner[] with industry and others to

---

[130] *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, at 15-17, (Apr. 16, 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[131] *NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NIST, at 1–2 (Apr. 2015), *available at* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf.

[132] *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, at 15-17, 28-29 (Apr. 16, 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[133] *See generally NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline*, NIST (May 2020), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf ("NISTIR 8259A").

tackle the pressing challenges of securing the technology supply chain" and "rely on private companies of all sectors and sizes, as well as government and academia, to contribute to the development of usable and effective domestic and global supply chain risk management practices."[134]

President Biden's Executive Order ("EO 14028") on "Improving the Nation's Cybersecurity" and his Administration's supply chain security initiatives also support a holistic voluntary framework.[135] Following a series of ransomware attacks targeting the United States' critical infrastructure, President Biden signed EO 14028 and charged multiple federal agencies with enhancing cybersecurity through various initiatives related to the security and integrity of the software supply chain. Notably and consistent with industry consensus, EO 14028 requires "the Federal Government to partner with the private sector," including federal contractors and service providers, to input identified issues and processes. EO 14028 has recognized that cyber vulnerabilities pose dynamic threats that must be continually monitored and mitigated. Among other things, EO 14028 seeks to remove obstacles to sharing threat information between the private sector and federal agencies and to identify IoT cybersecurity criteria for a consumer labeling program.[136] Under this program, the Secretary of Commerce acting through the Director of NIST is required to establish IoT cybersecurity criteria reflecting "increasingly comprehensive levels of testing and assessment program[s]" an IoT device may have undergone, based on a review of all relevant information,

---

[134] *U.S. Secretary of Commerce Gina Raimondo and Congresswoman Lizzie Fletcher Hold Roundtable with Energy Leaders on Addressing Cybersecurity Threats*, U.S. DEPARTMENT OF COMMERCE (Sep. 1, 2021), *available at* https://www.commerce.gov/news/press-releases/2021/09/us-secretary-commerce-gina-raimondo-and-congresswoman-lizzie-fletcher.

[135] *See Executive Order 14028 on Improving the Nation's Cybersecurity*, 86 FR 26633 (May 12, 2021), available at https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity ("EO 14028").

[136] EO 14028, Sec. 4(t).

labeling, incentive programs, and best practices.[137] EO 14028 further explains that the focus of the review is on "ease of use for consumers and a determination of what measures can be taken to maximize manufacture participation."

What EO 14028 does not do, nor do any of the implementation regulations and guides purports to do, is to single out a small group of manufacturers based solely on their identities. This is because categorical bans and blacklists will provide only an illusion of security.[138] EO 14028 thus marked a welcome change as the Administration recognized that a more fact-based holistic approach to cybersecurity is the foundation of sustainable, efficient, and effective development of the cybersecurity industry and related industries. Instead of focusing on the identity and origination of the equipment, the Commission should realign its efforts to promote a holistic risk-based approach to security. During President Biden's recent meeting with industry leaders discussing supply chain security initiatives, he recognized that the Federal government cannot address

---

[137] *Id.*

[138] *See, e.g.*, Daniel Ikenson, *Cybersecurity of Protectionism? Defusing the Most Volatile Issue in the U.S.-China Relationship*, CATO Institute Policy Analysis 815 (Jul. 13, 2017), available at https://object.cato.org/sites/cato.org/files/pubs/pdf/pa815.pdf ("If cybersecurity is the real objective, there are far less intrusive approaches that are much more likely to keep us secure. A cybersecurity regime that weds best business practices with valid statistical methods and implements the right combination of carrots and sticks could be the right solution."); Bruce Schneier, *Banning Chinese Phones Won't Fix Security Problems With Our Electronic Supply Chain*, THE WASHINGTON POST (May 8, 2018), available at https://www.washingtonpost.com/news/posteverything/wp/2018/05/08/banning-chinese-phones-wont-fix-security-problems-with-our-electronic-supply-chain (security technologist noting that "[i]t's doubtful this ban will have any real effect"); John C. Tanner, *Supply Chain Security is A Major Issue That Vendor Bans Won't Fix*, DISRUPTIVE ASIA (Oct. 8, 2018), available at https://disruptive.asia/supply-chain-security-major-issue/ ("[T]he political posturing over Huawei, ZTE and national security is not only paranoid populist pandering, it's also a distraction from a much larger problem that it doesn't come anywhere close to solving."); Tim Rühlig and Maja Björk, *What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe*, SWEDISH INSTITUTE OF INTERNATIONAL AFFAIRS (Jan. 2021), available at https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2020/ui-paper-no.-1-2020.pdf ("the idea of banning Huawei stems, rather than from concerns over network security, from a geopolitical logic.").

cybersecurity threats alone and invited participants to partner with the U.S. government to "bolster the nation's cybersecurity in partnership and individually."[139]

Similarly, expert advisors to the Commission have long echoed the importance of a risk-based approach to security. The Communications Security, Reliability and Interoperability Council ("CSRIC") has previously provided iterations of guidance and best practice recommendations to the Commission. The message from the CSRIC has been clear and loud – that the Commission should encourage industry to promote a voluntary, risk-based approach to address supply chain cybersecurity risk, including security-by-design principles and processes, not blacklisting particular companies. In March 2015, following an effort by over 100 cybersecurity experts from the communications sector, the federal government, state governments, equipment manufacturers, cybersecurity solution providers, and the financial, banking, and energy sectors, CSRIC IV unanimously adopted a detailed report that includes segment-specific analysis of the application of the NIST Cybersecurity Framework.[140] Then, in March 2016, CSRIC V Working Group 6 delivered a set of voluntary best practices for carriers to use when working with vendors and suppliers to reduce cybersecurity risks within the core network and found that "the NIST [Cybersecurity Framework] presented the strongest foundation for best practices."[141] Subsequently, in December

---

[139] *FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity*, THE WHITE HOUSE (Aug. 25, 2021), available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity.

[140] *The CSRIC IV Working Group 4 Report on Cybersecurity Risk Management and Best Practices*, CSRIC (Mar. 18, 2015), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[141] *The CSRIC V Working Group 6 Report on Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network*, CSRIC (Mar. 16, 2016), *available at* https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_FINAL_%20wAppendix_0316.pdf. The CSRIC V Working Group 6 released a final report in September 2016 which is available at: https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_Final_091416.docx.

2018, CSRIC VI Working Group recognized that "[r]estrictions on suppliers in the communication ecosystem, or any industry ecosystem for that matter, can have unintended consequences that need to be fully understood" and urged the Commission to refrain from adopting any mandatory framework but to work with CSRIC to "support the NIST collaborative process to define the voluntary procedures and identify the informed references for inclusion in updates to the Cyber Security Framework."[142] Likewise, the CSRIC VII working group in 2020 reiterated the Commission's previous recommendations to continue to participate in conversations and programs representing "strong public and private partnerships."[143]

Other current or former U.S. government officials also agree that there are better alternatives to achieving cybersecurity than categorical bans on specific providers. For example, Rear Admiral David Simpson, former Chief of the Commission's Public Safety and Homeland Security Bureau , has said that "banning one company's gear won't keep our data safe."[144] Instead, Admiral Simpson has advocated that "a stronger approach would be one in which we seek to improve our expectation for companies in the ICT ecosystem market and have them develop supply chain risk programs and work within industry verticals to develop supply chain risk clearing house arrangements, which in turn become third party accreditation organizations with standing relationships to

---

[142] *The CSRIC VI Working Group 3 Addendum to Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks*, CSRIC, at 3 (Dec. 13, 2018), *available at* https://www.fcc.gov/file/14855/download; *see also* CSRIC VI Working Group 3 Final Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks (Sept. 28, 2018), *available at* https://www.fcc.gov/file/14500/download.

[143] *The CSRIC VII Working Group 2 Report on Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation*, CSRIC, at 57-58 (Jun. 10, 2020), *available at* https://www.fcc.gov/file/18918/download.

[144] Tom Wheeler and David Simpson, *We Can't Secure 5G Networks by Banning Huawei Gear*, DEFENSEONE (Sept. 11, 2019), https://www.defenseone.com/ideas/2019/09/we-cant-secure-5g-networks-banning-huawei-gear/159795/.

the interagency supply chain risk centers of excellence."[145] Similarly, Wayne Jones, Chief Information Officer at the National Nuclear Security Administration, previously commented that "instead of banning software with a connection to China or other U.S. cyber adversaries, government tech shops should focus on installing safeguards that mitigate any risk the software poses for foreign spying or sabotage."[146] In the same vein, Department of Homeland Security and National Security Telecommunications Advisory Committee leaders have noted that a closer examination of information and communications technology ("ICT") products is preferable to excluding products based on their country of origin.[147]

Industry participants have also supported a holistic, risk-based approach, as the Commission's technical advisor and government officials recommended, in lieu of categorical bans and blacklists. As the Consumer Technology Association ("CTA") summarized in a March 2021 white paper,[148] government, industry, and consumers should all work together to promote better cybersecurity practices. Consistent with Huawei's recommendation, CTA encourages a risk-based approach to cybersecurity, and "neither the new Administration nor Congress should embrace rules,

---

[145] Charlie Mitchell, *Adm. Simpson: "Heavy-Handed' ICT Supply-Chain Plan Could Undermine Innovation*," INSIDE CYBERSECURITY, (Nov. 27, 2019), https://insidecybersecurity.com/daily-news/adm-simpson-%E2%80%98heavy-handed%E2%80%99-ict-supply-chain-plan-could-undermine-innovation.

[146] Joseph Marks, *The Government Should Be Focused On Mitigating The Danger Any Software Can Pose, Rather Than Banning Software From China And Elsewhere, The NNSA CIO Says*, NEXTGOV (June 28, 2018), https://www.nextgov.com/cybersecurity/2018/06/banning-software-isnt-route-cybersecurity-nuclear-security-agency-official-says/149385/.

[147] Mariam Baksh, *Leader On Presidential Panel Says Telecom Equipment Should Be Tested, Certified To Manage Supply-Chain Risks*, INSIDE CYBERSECURITY (Nov. 20, 2018), https://insidecybersecurity.com/daily-news/leader-presidential-panel-says-telecom-equipment-should-be-tested-certified-manage-supply.

[148] *Smart Policy to Secure our Smart Future: How to Promote a Secure Internet of Things for Consumers*, CONSUMER TECH. ASS'N (Mar. 2021), *available at* https://www.cta.tech/Resources/Newsroom/Media-Releases/2021/March/IOT-Device-Security-White-Paper-Release ("*CTA Cybersecurity White Paper*").

product labels or certification regimes for consumer IoT."[149] CTA believes the driver behind device innovation and enhancement of cybersecurity capability is a "light-touch regulatory approach" because only such an approach can keep up with the challenges associated with "rapidly changing technology and dynamic threats and attack techniques."[150] Moreover, as CTA rightly pointed out, a unilateral mandatory approach such as the one advocated by the Commission's proposed rules will only cause "possible impacts on global trade commitments," "be disruptive and impose substantial burdens on manufacturers well beyond the few covered entities," and "be difficult to implement for manufacturers across the supply chain."[151] Similarly, the Rural Broadband Alliance ("RBA"), a trade association of rural broadband service providers, has spoken out against the Commission's approach to exclude any single vendor or set of vendors from participating in the U.S. carrier network as a proposal that "does little to address the actual risks from the basis of the FCC's primary threat concerns."[152] The RBA then offered CSRIC's recommendations as "a logical starting point to improve security" followed by a framework based on "the voluntary approach embodied by the NIST Cybersecurity Framework … and available technical approaches . . . to drive future development of security-by-design standards and best practices."[153] The RBA also provided additional recommendations for consideration, including the use of trusted third-parties to "conduct deep independent analysis of all software and firmware (including source code)

---

[149] *CTA Cybersecurity White Paper*, at 7-13.

[150] *CTA Cybersecurity White Paper*, at 4-5.

[151] Comment of Consumer Technology Association, ET Docket No. 21-232, EA Docket No. 21-233 (Filed Jun. 11, 2021).

[152] Comment of Rural Broadband Alliance, WC Docket No. 18-89 (Filed Jun. 1, 2018) ("Rural Broadband Comment").

[153] Rural Broadband Comment, at 6-7.

of all network gear that will be used by wireless carriers."[154] In addition, the Alliance for Telecommunications Industry Solutions' recent white paper on 5G Supply Chain Standard stated that "[f]rom a holistic standpoint, the 5G supply chain must be considered within the larger context of securing 5G infrastructure, which includes cybersecurity threats and supply chain vulnerabilities."[155]

Last but not least, there is broad consensus across standard setting organizations on the benefits of a holistic, risk-based approach to address cybersecurity. The Network Equipment Security Assurance Scheme ("NESAS"), for example, is an industry-wide security assurance framework jointly developed by 3GPP and GSMA to facilitate improvements in security levels across the mobile industry.[156] NESAS does not outright rejects an equipment by its identity or country of origin. Rather, NESAS allows equipment manufacturers, network operators, and regulators to define and apply secure design, development, implementation, and product maintenance processes.[157] In turn, equipment manufacturers can demonstrate the established processes to external independent security auditors to assess compliance. Additionally, equipment manufacturers submit network equipment products to security laboratories against security requirements defined by

---

[154] Rural Broadband Comment, Ex. 1 (Domain5 Recommendation), at 7-8.

[155] *See ATIS 5G Supply Chain Standard Creating the Foundation for Assured 5G Networks*, ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS, at 5 (Sept. 2021) available at https://www.atis.org/resources/atis-5g-supply-chain-standard.

[156] *See generally FS.13 – NESAS Overview v.2.0.*, THE GSM ASSOCIATION (Feb. 5, 2021), available at https://www.gsma.com/security/resources/fs-13-network-equipment-security-assurance-scheme-overview.

[157] *See generally FS.15 – NESAS Development and Lifecycle Assessment Methodology v.2.0*, THE GSM ASSOCIATION (Feb. 5, 2021), available at https://www.gsma.com/security/resources/fs-15-network-equipment-security-assurance-scheme-vendor-development-and-product-lifecycle-requirements-and-accreditation-process.

3GPP so that information about equipment's level of security can be forwarded to operators and regulators.[158]

B. The Commission's Inquiries into Enhancing Cybersecurity and Security-by-Design for 5G Networks Are Not New.

Categorical bans provide little actual security and ignore the policies and recommendations adopted by the U.S. government, supporting a holistic risk-based approach to security. As a leading global provider of ICT infrastructure and smart devices, Huawei's mission is to establish and improve the ICT industry and ecosystem through collaboration and innovation. Together with industry partners worldwide and in the U.S., Huawei has been supporting and will continue to support the Commission's effort to develop a secure ICT sector, including the RF equipment industry, by participating in the various rulemaking, standard setting, and research and development activities, notwithstanding its unwarranted inclusion to the Covered List.

From a cyber security perspective, threats often come from external and internal actors whose capabilities are rapidly improving. From a data privacy point of view, the increased digitalization of business and social transactions is creating new opportunities for malicious actors to breach the data integrity of organizations, allowing them to exploit personal or critical information for fraud, espionage, and sabotage. The Commission should recognize the complex nature of the challenges from cyber security and data privacy issues, building on its previous views and understandings of the cybersecurity issue in other proceedings. To that end, Huawei notes that the Commission's inquiries into enhancing cybersecurity and security-by-design for advanced communications networks and equipment are not new.

---

[158] *See generally FS.14 – NESAS Security Test Laboratory Accreditation v.2.0*, THE GSM ASSOCIATION (Feb. 5, 2021), available at https://www.gsma.com/security/resources/fs-14-network-equipment-security-assurance-scheme-security-test-laboratory-accreditation.

For example, in 2015, the Commission issued a Notice of Proposed Rulemaking on the proposed millimeter wave ("mmW") bands above 24 GHz for the provision of Fifth Generation or "5G" mobile radio services ("2015 mmW NPRM"),[159] seeking comments on "how to ensure that effective security features are built into key design principles for communications devices and networks."[160] The Commission adopted requirements that mmW band licensees provide high-level descriptions of how confidentiality, integrity, and availability principles are reflected in their network security design before commencing operations.[161] Specifically, mmW band licenses were required to disclose: a general description of the licensee's anticipated approach to assessing and mitigating cyber risk; the cybersecurity standards and practices to be deployed; a description of the licensee's participation in standards bodies or industry-led organizations; and other information about approaches to security the licensee intends to offer and plans to incorporate outputs from the Information Sharing and Analysis Organizations as elements of the licensee's security architecture. The FCC correctly found that these reporting requirements will help ensure that industry focuses attention throughout the development and deployment processes on the most effective ways to include security safeguards at the earliest possible points, and would keep the FCC informed of ongoing progress to provide timely, measured, and effective responses to emerging issues.[162] Although these requirements were subsequently withdrawn, they offer a practical holistic framework to address the cyber security concerns raised in the instant NOI.

---

[159] *See Use of Spectrum Bands Above 24 GHz For Mobile Radio Services et al.*, GN Docket No. 14-177, Notice of Proposed Rulemaking, FCC 15-138 (rel. Oct. 23, 2015) ("2015 mmW NPRM").

[160] 2015 mmW NPRM, ¶ 4.

[161] *See Use of Spectrum Bands Above 24 GHz For Mobile Radio Services, et al.*, Report and Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 8014, ¶¶ 262-65 (2016).

[162] *Id.*, ¶ 265.

Following the 2015 mmW NPRM, the Commission launched a Notice of Inquiry in 2016 ("5G Security NOI") to "*look[] holistically* at the security implications (*e.g.*, as to IoT) that arise through the provision of a wide variety of services to various market sectors and users in the future 5G network environment," in addition to "explor[ing] 5G security threats, solutions, and best practices."[163] In doing so, the Commission clarified that it was not conducting the NOI in a vacuum.[164] Instead, the Commission launched the NOI with the intent to complement the "important work on cybersecurity that is already taking place within the government and private sector."[165] The 5G Security NOI also explored "5G security threats, solutions, and best practices"[166] and encouraged commenters to consider a common thread throughout the NOI. That is, "how can we, working together with other stakeholders, ensure the rapid deployment of secure 5G networks, services, and technologies?"[167]

Although the 5G Security NOI was subsequently rescinded,[168] it still provides a targeted and valuable approach for examining issues of cybersecurity in 5G networks and asks the right questions as to "how 5G service providers and equipment manufacturers can ensure the critical security software updates are installed on their subscriber devices in a timely fashion?" and "ensure firmware and software patch management related to security through their customer relationships?"[169] It also asked how IoT devices could place 5G networks at risk and what roles network

---

[163] *Fifth Generation Wireless Network and Device Security*, Notice of Inquiry, PS Docket No. 16-353, 31 FCC Rcd 13110, ¶¶ 1, 6 (rel. Dec. 16, 2016) ("*5G Security NOI*") (emphasis added).

[164] *5G Security NOI*, ¶ 4.

[165] *Id.*

[166] *5G Security NOI*, ¶ 6.

[167] *5G Security NOI*, ¶ 8.

[168] *Fifth Generation Wireless Network and Device Security*, Order, DA Docket No. 17-131, 2 FCC Rcd 1106 (rel. Feb. 3, 2017).

[169] *5G Security NOI*, ¶ 24.

equipment providers, ISPs, and device manufacturers play to mitigate the risks.[170] Similar to the 5G Security NOI, the Commission should craft questions to encourage all stakeholders in the communications supply chain to provide cybersecurity best practices and guidelines to secure communications networks.

C. The Commission Should Leverage Prior Efforts to Build and Enhance Cybersecurity and Address the Particular Security Risks.

The concerns about categorical bans on certain equipment providers apply equally to the Commission's forced revocation proposal and demonstrate that the Commission's failure to consider a holistic risk-management alternative is arbitrary and capricious. Rather than adopting any new mandatory framework for equipment authorization security requirements using questionable legal authority, the Commission should reinvigorate prior efforts to leverage voluntary means of securing 5G networks and devices. Huawei would fully support such efforts.

For example, in the Spectrum Frontiers NPRM,[171] which had the support of then-Commissioner Rosenworcel,[172] Huawei noted that "security and privacy features for 5G systems cannot be built on top of the system design; rather they must be built into the system design" and otherwise encouraged including security protection at an early stage of 5G development.[173] Huawei also noted that systems are in need of a "secure architecture, stringent identity management and data

---

[170] *5G Security NOI*, ¶ 33.

[171] *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services et al.*, Second Report and Order, Second Further Notice of Proposed Rulemaking, Order on Reconsideration, and Memorandum Opinion and Order, GN Dockt No. 14-177, 32 FCC Rcd 10988, ¶¶ 110-13 (2017) ("*Spectrum Frontiers NPRM*").

[172] Statement of Commissioner Jessica Rosenworcel, GN Docket No. 14-177, *available at* https://docs.fcc.gov/public/attachments/FCC-16-89A4.pdf.

[173] Comments of Huawei, 23, GN Docket No. 14-177 (filed Jan. 28, 2016) (quoting Huawei, 5G Security: Forward Thinking at 24 (2015)), *available at* https://ecfsapi.fcc.gov/file/60001416250.pdf ("Huawei mmW Comments").

protection, more rigorous authentication methods, and an array of system-level protections to defend against distributed denial of service ('DDOS') attacks and other intrusions."[174]

After analyzing the record and the comments received, the Commission adopted Huawei's recommendations to focus on security in the development stage rather than after network deployment. The Commission concluded that it can "best facilitate the adoption of security-by-design approaches by promoting an open dialogue about security practices that would be consistent with a discussion at a standards organization"[175] and that this holistic approach not only recognizes that the private sector is in the best position to evaluate and address risks to their network operations but also "reduces the need for ongoing regulatory involvement in private sector security practices."[176]

The Spectrum Frontiers NPRM also led the Commission to issue the 5G Security NOI, which was subsequently rescinded[177] only because then-FCC Chairman Ajit Pai believed the Commission "lack[s] the expertise and authority to dive headlong into this issue, and I don't think any agency should take a band-by-band approach to cyber. These are issues that are better left for security experts to handle in a more comprehensive way."[178] The Commission should revive its prior effort and consider a holistic approach to cybersecurity.

Finally, in considering and evaluating the Commission's prior efforts to ensure a secure communications network, the Commission should already be on alert that its mandatory removal

---

[174] Huawei mmW Comments at 24.

[175] *Spectrum Frontiers NPRM*, ¶ 262.

[176] *Spectrum Frontiers NPRM*, ¶ 255.

[177] *Fifth Generation Wireless Network and Device Security*, Order, PS Docket No. 16-353 (rel. Feb. 3, 2017).

[178] *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services*, Statement of Commissioner Pai, GN Docket No. 14- 177, p. 275.

and replacement of equipment and services on the Covered List has caused more cost, disruption, and uncertainty for affected small carriers. An agency must consider "an important aspect of the problem" and "must cogently explain why it has exercised its discretion in a given manner."[179] That means that an agency's "failure to consider … alternatives, and to explain why such alternatives were not chosen, [is] arbitrary and capricious."[180] The Commission's proposed rules and revocation mandate represent another highly unusual step guaranteed to harm a much broader base of U.S. consumers, businesses (including small businesses), and manufacturers. Rather than continuing the erroneous path of focusing on the origin of the equipment and supplier to introduce further disruption to the supply chain, the Commission should consider reasonable alternatives, including the use of a holistic approach to cybersecurity, limit the revocation of authorization to equipment that it believes interferes with the RF communications network. As described throughout these comments, the abundant alternatives available to the Commission highlight the Commission's failure to consider "significant and viable and obvious alternatives."[181]

VI. CONCLUSION

For the foregoing reasons, the Commission should not adopt the proposed rules and instead use the information received in response to the Notice of Inquiry to formulate vendor-neutral equipment security standards.

---

[179] *See Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 48 (1983).

[180] *Int'l Ladies' Garment Workers' Union v. Donovan*, 722 F.2d 795, 815 (D.C. Cir. 1983).

[181] *Dist. Hosp. Partners, L.P. v. Burwell*, 786 F.3d 56, 59 (D.C. Cir. 2015).

Respectfully submitted,

s/ Andrew D. Lipman

Dennis J. Amari
Vice President, Federal & Regulatory Affairs

Donald A. (Andy) Purdy, Jr.
Chief Security Officer

Huawei Technologies USA, Inc.
1101 16th Street, NW., Suite 401
Washington, DC 20036

Andrew D. Lipman
JiaZhen (Ivon) Guo

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
ivon.guo@morganlewis.com

Counsel to Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc.

September 20, 2021